Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 24 June 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Boston Globe reports Massachusetts's online records pose a risk, with tax liens, mortgage papers, deeds, and other real estate−related documents publicly available in online databases run by registries across the state. (See item 7)
- The New York Times reports a 20−year−old man stole a Cessna 172 Skyhawk from the Danbury Municipal Airport and flew it drunk to New York's Westchester County Airport, showing the need for tighter security at small airports. (See item 10)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 23, ISO New England, New York Independent System Operator, and PJM Interconnection* — **Independent System Operators to coordinate on natural gas supply conditions related to generation.** The three northeastern regional grid operators have agreed to collaborate to ensure electric power system reliability in the event of constraints on the natural gas supply system. ISO New England, New York Independent System Operator and PJM Interconnection will coordinate operations and practices and share information and technology during periods of extreme cold weather and/or abnormal natural gas supply or delivery conditions. Natural gas−fired electric generation accounts for much of the generating capacity in the three regions. "As the electricity industry grows more dependent on natural gas as a primary fuel source for

generating resources, it's critical the three northeast grid operators coordinate closely to ensure reliability is maintained when extraordinary power system conditions occur," said Gordon van Welie, ISO New England president and chief executive officer. Periods of extreme cold weather place heavy demands on both the electric and natural gas transmission systems as energy consumption increases. Sometimes, the resulting delivery restrictions on the gas pipeline system can limit the ability of gas−fired generation to produce electricity.
Source: http://www.pjm.com/contributions/news−releases/2005/20050623−northeast−iso−rto−gas−mou.pdf

2. *June 23, Agence France−Presse* — **Tokyo promises tighter control after nuclear power plant data leak.** Japan's government vowed to tighten controls on information at nuclear power plants after confidential data on at least two facilities was inadvertently leaked over the Internet. "As nuclear plants are important facilities in terms of preventing terrorism ... we want to take thorough measures about information management," Chief Cabinet Secretary Hiroyuki Hosoda said on Thursday, June 23. Hosoda said the government believed the leak did not involve any crucial information on nuclear materials from the Tomari nuclear power plant in northern Japan and the Sendai plant in southern Japan. Major electrical machinery maker Mitsubishi Electric Corp earlier said confidential data from two nuclear power plants had been leaked over the Internet from a virus−infected computer used by an employee at a group firm. The employee was in charge of nuclear inspections. His computer was infected with a virus that reveals data through the Winny file−sharing software. Jiji Press said the leaked data included lists of plant workers' names, detailed inspection results and pictures of inside the plants.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050623/sc_afp/japannuclearitscandalmitsubishicompany_050623112114

3. *June 23, East Valley Tribune (AZ)* — **Premature record power demand in Phoenix has commissioners questioning readiness.** Record electricity use in the Phoenix, AZ, area is prompting two members of the Arizona Corporation Commission (ACC) to seek assurances from utilities that they are prepared to deal with what looks like will be a long, hot summer of electric demand. In separate letters sent to utility executives of Arizona Public Service (APS) and Salt River Project (SRP) on Wednesday, June 22, commission Chairman Jeff Hatch−Miller and commissioner Kris Mayes said electric demand hit a record Tuesday, June 21, which is unusually early in the summer air conditioning season. Peak demand usually doesn't occur until July or August. In a letter to APS President Jack Davis, Mayes questioned whether the utility had underestimated peak demand this summer. According to figures provided by the ACC and the utilities, the peak electric use in the Phoenix area by customers of APS and SRP reached a record 10,200 megawatts Tuesday. The utilities thought peak demand could reach as high 10,600 megawatts on Wednesday, but lower than expected temperatures and humidity caused the demand to peak at about the same level as Tuesday. The utilities have projected that the peak demand this summer will hit about 10,860 megawatts.
Source: http://www.eastvalleytribune.com/index.php?sty=43506

4. *June 23, New York Times* — **Chinese oil giant in takeover bid for U.S. corporation.** One of China's largest state−controlled oil companies made a $18.5 billion unsolicited bid Thursday, June 23, for Unocal, signaling the first big takeover battle by a Chinese company for an American corporation. The bid, by the China National Offshore Oil Corporation (CNOOC), may be a watershed in Chinese corporate behavior, and it demonstrates the increasing influence

on Asia of Wall Street's bare−knuckled takeover tactics. The offer is also the latest symbol of China's growing economic power and of the soaring ambitions of its corporate giants, particularly when it comes to the energy resources it needs desperately to continue feeding its rapid growth. CNOOC's bid, which comes two months after Unocal agreed to be sold to Chevron, the American energy giant, for $16.4 billion, is expected to incite a potentially costly bidding war over the California−based Unocal, a large independent oil company. Unocal said in a statement that its board would evaluate the offer, but that its recommendation of the deal with Chevron remains in effect.
Source: http://www.nytimes.com/2005/06/23/business/worldbusiness/23u nocal.html?

5. *June 22, Newsday (NY)* — **New York utility projects adequate supplies for summer.** The Long Island Power Authority (LIPA) said on Wednesday, June 22, that it will have enough electricity to meet demand this summer. In releasing the utility's annual summer power outlook report, chairman Richard Kessel said LIPA has "an adequate supply of electricity to meet both normal and extreme summer demands." Kessel said that during periods of extreme heat and humidity, the electricity demand could exceed 5,670 megawatts. However, LIPA will have 6,136 available, including 159 megawatts of new peak generation capacity that will come online by July 1. While there shouldn't be a problem this summer, Kessel said, "looking ahead several years, we'll still need to add more resources to keep up with demand and provide a wider margin should a major power plant or cable connection fail to operate when needed most." He said the average household electricity use on Long Island has increased by 15 percent during the past six years, and he urged customers to expand their conservation efforts.
LIPA press release with graphics:
http://www.lipower.org/newscenter/pr/2005/june22.summer.html
Source: http://www.newsday.com/news/local/longisland/ny−lilipa0623,0 ,141593.story?coll=ny−top−headlines

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *June 23, Press Association (UK)* — **UK police investigate call center breaches.** A call center worker in Delhi, India, sold the bank account details of 1,000 British customers to a newspaper journalist, it was reported Thursday, June 23. The details have emerged on the same day that police launched an investigation into alleged call center security breaches. The City of London Police began an investigation after receiving a dossier of information from a newspaper

journalist outlining a number of banks whose security may have been compromised. An undercover reporter was sold information on a thousand accounts and the numbers of passports and credits cards for about $7.75 each. The information received included account holders' secret passwords, addresses, phone numbers and credit card, passport and driving license information. The information could allow criminals to access the financial details of unwitting victims and lead to the raiding of accounts and the cloning of credit cards.
Source: http://www.guardian.co.uk/business/story/0,3604,1512665,00.h tml

7. *June 23, Boston Globe* — **Massachusetts's online records pose risk.** Tax liens, mortgage papers, deeds, and other real estate−related documents are publicly available in online databases run by registries of deeds across Massachusetts. Staff of the Boston Globe found documents in free databases of all but three Massachusetts counties containing the names and Social Security numbers of Massachusetts residents. Public documents that sometimes contain names and Social Security numbers include state and federal tax liens, Massachusetts Health liens, child support liens, and, less frequently, mortgages. Although registers of deeds said that they are unaware of cases in which criminals used information from their databases maliciously, the information contained in the documents would be more than enough to steal an identity and open new lines of credit, said Eric Bourassa, a consumer advocate with the Massachusetts Public Interest Research Group who deals with identity theft issues. Registers of deeds said that the databases are normally used by real estate professionals, commercial users such as mortgage lenders, and members of the general public who want to ensure that certain documents have been filed.
Source: http://www.boston.com/business/technology/articles/2005/06/23/states_online_records_pose_risk/?mode=PF

8. *June 23, New York Times* — **Bank in Utah says its data was at risk in intrusion.** A small bank in Utah is the latest company to become entangled in the controversy over a security breach that has put personal data on 40 million cardholders at risk for fraud. The Utah institution, Merrick Bank, began using CardSystems Solutions, the processor from which the information was stolen, when it bought a portion of Provident Bank's merchant business in November 2004. Merrick acknowledged on Wednesday, June 22, that CardSystems had not complied with Visa and MasterCard's security standards, but would not say when it became aware that the company was not following the rules, or whether the violations occurred under its watch. In a statement, Merrick said it was "committed to ensuring that all the necessary steps are taken by CardSystems to quickly resolve the problems that allowed the incident to occur." Merrick said that CardSystems had already made a number of changes, and with the help of an outside security consultant would complete any remaining changes shortly. Merrick's disclosure raises more questions about the oversight of security controls in an industry where processing companies are largely unregulated, even though they handle millions of consumer records each day.
Source: http://www.nytimes.com/2005/06/23/business/23cards.html

9. *June 23, MSNBC* — **Identity theft concerns grow.** In one of the most extensive studies yet on consumer attitudes about identity theft, research group Gartner Inc. found that about half those polled either weren't aware they were entitled to a free credit report or considered them "not effective" in fighting identity theft. The survey, released Thursday, June 23, also found that one−third of consumers are very concerned about being victims of identity theft, and nearly half

are altering their online activities as a result. Gartner researcher Avivah Litan, who led the study, said the survey results also suggested that more than one million consumers have been tricked into divulging their personal information to senders of so−called phishing e−mails, with financial losses totaling nearly $1 billion. Identity anxiety is also hampering e−commerce growth, the study found. Forty−two percent of respondents said worries about phishing, data losses, and spyware are affecting their online shopping habits. "Consumers are really getting scared, and they don't think their government is protecting them," said Litan.
Gartner: http://www.gartner.com
Source: http://msnbc.msn.com/id/8322300/

[Return to top]

Transportation and Border Security Sector

10. *June 23, New York Times* — **Police say 20−year−old stole a plane and flew it drunk.** The first hint that something was amiss early Wednesday, June 22, at New York's Westchester County Airport was the erratic motion of the low−flying Cessna. Moments later security workers approached the aircraft and beer cans fell out of the cabin as the pilot opened the door. The bizarre airborne capert set county and law enforcement officials into a frenzy of finger−wagging, with September 11−style alarms over airport security. According to Thomas Belfiore, commissioner of the Westchester County Department of Public Safety, the 20−year−old pilot, Philippe Patricio of Bethel, CT, stole the airplane from the Danbury Municipal Airport in Connecticut and took two friends, both 16, on a joy ride. Low on gas and lost, Patricio, whose blood−alcohol level, 0.15, was almost twice the legal limit for driving a car, happened to find the county airport even though it was closed because of construction and the runway lights were off. The biggest mystery centered on how he gained access to the Cessna 172 Skyhawk in the first place. The Westchester County executive, Andrew J. Spano, said the incident showed the need for tighter security at small airports like Danbury. Westchester County Airport, northeast of White Plains, requires all planes to be outfitted with boots, or wheel locks.
Source: http://www.nytimes.com/2005/06/23/nyregion/23plane.html

11. *June 23, Associated Press* — **Plane traveling from Chicago makes emergency landing in Colorado.** A United Airlines plane en route to Las Vegas from Chicago declared an emergency and made an unscheduled landing at Pueblo Memorial Airport Wednesday, June 22, after its crew initially reported smoke in the cockpit, an airport official said. None of the 156 people aboard Flight 1525 were injured, airport manager Jerry Brienza said. Passengers waited at least four hours for another airplane to arrive. Karen Byrd, of the Federal Aviation Administration, said the crew reported a vibration in the cabin. Brienza said the crew reported smelling smoke but later said it was a problem with some avionics equipment in the cockpit.
Source: http://www.usatoday.com/travel/flights/2005−06−23−ual−emerge ncy_x.htm

12. *June 23, USA TODAY* — **Four major airlines increase fares.** The four biggest U.S. airlines −− American, United, Delta and Northwest −− raised most airfares Wednesday, June 22, citing record−high fuel prices. United raised fares 3% across the board, Northwest raised domestic fares 3%, and American and Delta raised fares $5 each way. Continental did not raise fares. The airfare increases come after a turbulent year in which big airlines have been plagued by higher

fuel costs, under funded pension obligations and fierce competition from discount carriers. Before Wednesday, domestic fares had risen seven times since February, especially on routes where major airlines face little competition from discount carriers. Meanwhile, fares to Europe are the highest that passengers have seen in years.
Source: http://www.usatoday.com/travel/news/2005−06−22−fares−usat_x. htm

[Return to top]

Postal and Shipping Sector

13. *June 23, DM News* — **House bill includes no Postal Service emergency preparedness funds.** The U.S. Postal Service (USPS) received no emergency preparedness funding in the $66.9 billion fiscal year 2006 Transportation, Treasury, Housing, and Urban Development bill that the House Appropriations Committee passed Tuesday, June 21. The bill provides $87.4 million for the USPS to meet its statutory obligation to provide free mail for the blind, free mailing of absentee balloting materials by members of the armed forces and other U.S. citizens residing abroad, and free mailing of balloting materials between state and local officials. It also appropriated $29 million as part of the Revenue Forgone Reform Act of 1993. In testimony before a subcommittee of the House Appropriations Committee in April, Postmaster General John E. Potter asked for three reimbursements: $29 million for revenue forgone, $108.5 million for statute−imposed costs, and $51 million for the cost of equipment to defend against biohazards in the mail. Potter said the $51 million would be used to deploy biohazard detection and ventilation and filtration systems and construct a mail irradiation facility in the Washington, DC, area. Potter also said the USPS currently spends about $800,000 of its own funds monthly to irradiate mail destined for Congress, the White House, and federal government agencies in Washington, DC.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3316 5

[Return to top]

Agriculture Sector

14. *June 23, Palm Beach Post (FL)* — **Citrus workers trained to spot canker.** More than 400 citrus grove owners and workers attended a training session in identifying citrus canker at the University of Florida's Indian River Research and Education Center. By the end of June, state and federal canker officials hope to train as many as 2,000 more pairs of eyes among those who already work in the groves to identify the disease, which causes brown, cork−like lesions on leaves, stems and fruit. Each attendee was given a laminated flow chart with photos of blemished leaves, showing how to determine visually whether a pockmark is canker or perhaps another plague such as citrus scab or greasy spot. The training sessions, which was given in Spanish and English at the center, were part of a series of six taking place around the state to teach workers to look for the disease's symptoms. Before the 2004 hurricanes, canker eradication program officials oversaw the removal of about two million citrus trees statewide. The disease broke out in Miami−Dade County in 1995. The storms of August and September spread the canker across the state, sharply increasing the incidences of the bacterial plague. About 4.2 million commercial trees, about four percent of the total, and nearly 800,000 trees in

residential areas have been removed or are scheduled to be by August 1.
Source: http://www.palmbeachpost.com/business/content/business/epaper/2005/06/23/a1d_canker_0623.html

15. *June 23, Natural Environment Research Council* — **Parasite threatens European fish.** A new deadly disease, carried by an invasive fish species, is threatening European fish diversity. Lead researcher Rodolphe Gozlan from the Center for Ecology & Hydrology (CEH) said: "We have found a parasite that may pose a severe threat to some freshwater fish species in Europe. This discovery has major biological implications and may have economic implications." The scientists working for CEH and the Center for the Environment, Fisheries & Aquaculture Science (CEFAS) have found an infectious disease carried by the topmouth gudgeon −− the most invasive fish species in Europe. The disease stops the European sunbleak, an endangered species in mainland Europe, from spawning −− leading to its rapid decline and possible eventual extinction. The scientists blame the disease for the rapid demise of the sunbleak in parts of Europe following the spread of the Asian topmouth gudgeon. "The new disease is already affecting other freshwater fish such as the fathead minnow and may affect native UK fish species," added Gozlan. The researchers found that the parasite does not harm the topmouth gudgeon. Gozlan said: "The topmouth gudgeon is a healthy host for this deadly parasite. This parasite could threaten commercial fisheries, including salmon farms."
Source: http://www.nerc.ac.uk/publications/latestpressrelease/2005−2 8parasitefish.asp

16. *June 23, Associated Press* — **African honeybees becoming established in Florida.** A University of Florida researcher says African bees are back in Florida and that could be bad news for the state's $16 million honeybee industry. Glenn Hall said African honeybees have been found and stopped at ports in Jacksonville, Miami, and Tampa since 1987. The Florida Department of Agriculture and Consumer Services would capture them in bait hives. But Hall notes the bees are here to stay due to the warm climate and could affect the beekeeping industry and the pollination of many crops. Hall says the Tampa area is seeing a small spread of them and the African bees are also being found farther inland from the ports.
Source: http://www.local10.com/news/4629397/detail.html

[Return to top]

Food Sector

17. *June 23, Reuters* — **Genetically modified foods can bring benefits, but vigilance needed.** Genetically modified (GM) foods can bring benefits both to farmers and consumers, but safety checks will always be needed before they are marketed, the World Health Organization (WHO) said on Thursday, June 23. As the debate rages in Europe on what are often branded there as "Frankenstein" foods, the WHO said there was no evidence to suggest that any foods currently on the market posed health risks. In a 58−page report, the WHO said GM organisms can increase crop yields and food quality, thereby improving health and levels of nutrition, as well as boost profits for farmers and industry. But since some of the genes used in GM crops have not been in the food chain before, the potential effects on health and society must always be assessed before they are grown and sold.
WHO report: http://www.who.int/foodsafety/biotech/who_study/en/index.htm l
Source: http://www.reuters.co.za/locales/c_newsArticle.jsp?type=topN

ews&localeKey=en_ZA&storyID=8872007

[Return to top]

Water Sector

18. *June 22, The Californian (CA)* — **Millions of gallons of water lost after plant malfunction.** A malfunction at a treatment plant Wednesday morning, June 22, sent nearly 11 million gallons of drinking water into a nearby creek, leading to some flooding and reductions in deliveries to water agencies in Southwest Riverside and San Diego counties. The malfunction happened about 9:15 a.m. (PDT) at the Robert A. Skinner water treatment plant near Lake Skinner east of Murrieta, CA. The break caused water to enter an emergency outflow pipe that empties into Tucalota Creek, Metropolitan Water District officials said. Water District spokesperson Denis Wolcott said that the malfunction happened when a gate leading from the treatment modules closed without warning, forcing water into an emergency relief valve. The cause of the malfunction is still being investigated, Wolcott added. Agencies receiving water from the plant include Eastern Municipal Water District and Western Municipal Water District in Riverside County and the San Diego County Water Authority. "This is one of the key treatment plants for San Diego County," Wolcott said.
Source: http://www.nctimes.com/articles/2005/06/23/news/californian/ 22_13_446_22_05.txt

[Return to top]

Public Health Sector

19. *June 23, Associated Press* — **Third North Carolina hospital received hydraulic fluid.** A third North Carolina hospital said Wednesday, June 22, that it received barrels that were supposed to contain a cleanser for surgical instruments but instead contained hydraulic fluid. A spokesperson for Wake Forest Baptist Medical Center said hospital workers caught the mistake immediately and no patients underwent surgery with instruments washed in the fluid. It was not immediately clear if there was a connection between the discovery at the Winston−Salem hospital and similar discoveries at two other hospitals. But all three hospitals used the same soap supplier, Cardinal Health of Dublin, OH. Wake Forest hospital spokesperson Mark Wright said that two loads of surgical equipment came out of a washer December 13 feeling greasy. Workers halted the cleaning and checked the barrels, which were supposed to contain cleanser but instead contained hydraulic fluid. Officials at the Winston−Salem hospital were unaware at the time that any other hospital had received barrels of hydraulic fluid, he said. For two months late last year, surgeons at Duke Health Raleigh Hospital and Durham Regional Hospital unknowingly used instruments on nearly 4,000 patients that had been washed with hydraulic fluid instead of soap. The error at the Duke hospitals happened after elevator workers drained hydraulic fluid into empty soap containers without changing the labels.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/23/AR2005062300057.html

20. *June 23, Billings Gazette (MT)* — **Hospital tests robot for assisting doctors.** Staff at St. Vincent Healthcare, in Montana, tested a robot on Wednesday, June 22, that puts physicians at

the bedsides of patients who are miles away. Using the RP6 −− or remote presence −− robot, a doctor in Billings could do rounds in a medical center in Scobey, stopping in each patient's room. The patient would hear and see the doctor through a flat screen monitor mounted on the robot. The doctor would view two screens −− one showing the patient and the other his medical records. RP6 played a role in a statewide bioterrorism disaster drill that focused on telemedicine. Medical providers in 30 communities participated in the drill, which simulated an outbreak of tuberculosis or the plague. The sites −− including St. Vincent Healthcare −− linked to one another and to the state Department of Public Health and Human Services through several interactive videoconference networks. If a disaster struck Montana, health care facilities across the state could use the telemedicine network to instantaneously share information. Physicians' expertise could also be shared. Montana has only a handful of infectious−disease specialists, and they would be in high demand during an outbreak. Doctors could also use a robot like the RP6 to enter rooms of contagious patients.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2005/06/23/build/local/30−robots.inc

21. *June 22, National Institute of Allergy and Infectious Diseases* — **Scientists unveil mechanism behind resistance to severe malaria.** Scientists have discovered why people with a specific type of hemoglobin −− the oxygen−carrying molecule that gives red blood cells their color −− are less prone to severe malaria. In a series of experiments, the researchers determined how hemoglobin type C impairs the ability of malaria parasites to cause disease symptoms. “This research gives us a new insight into malaria, a major global killer that claims a life every 30 seconds,” notes Anthony S. Fauci, director of the National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health, where the research was conducted. “If we better understand the natural protective mechanisms against malaria, we might be able to mimic that protective effect through vaccines or drugs,” says NIAID researcher Thomas E. Wellems. Hemoglobin exists in several varieties. Hemoglobin A is the most common, but in parts of West Africa, where malaria is rife, one−fourth of the population has at least one gene for hemoglobin C. Children with at least one hemoglobin C gene are less prone to deadly cerebral malaria, in which parasite−infected red blood cells accumulate in the brain. But how hemoglobin C confers this protection has puzzled scientists until now.
Source: http://www2.niaid.nih.gov/newsroom/Releases/wellems_malaria. htm

[Return to top]

Government Sector

22. *June 23, Associated Press* — **Subterranean visitor center taking shape in shadow of Capitol dome.** Fifty feet below ground and steps from the U.S. Capitol, dozens of construction workers haul bricks and cement, lay marble and tiles and put other finishing touches on a subterranean project almost as large as the building itself. When completed, the three−level catacomb will be a place to welcome Capitol visitors and make lawmakers safer in doing their business. Slated to open in September 2006, the Capitol Visitor Center will be the ninth and, by far, largest addition to the building in its history. Inside the center, an exhibition gallery twice as big as the Capitol Rotunda, the circular room beneath the dome, will aim to demystify Congress for the 10,000 people who tour the building daily. Other portions of the addition, all off−limits to the public, include an auditorium for lawmakers that can substitute as a working chamber should

either of the existing ones need to be closed, and extra workspace for the House and Senate, congressional hearings and the news media. Besides the add−ons for lawmakers, the center will help ease the wait for Capitol visitors, who have had to line up outside for hour long tours of the building. Once through security, they will be free to roam the three−level facility. Security was one reason for building the center, but the main issue was that "visitors were not being treated with respect when they came here," said Alan Hantman, the architect.
Source: http://www.newsday.com/travel/ny−trcapitol0521,0,1110478.story?coll=ny−travel−datelines

[Return to top]

Emergency Services Sector

23. *June 23, Patriot−News (PA)* — **Officials to replace emergency radio network.** Emergency responders many times can't rely on getting their messages out on hand−held walkie−talkies, known as "portables," especially if they're inside a building or in areas distant from towers, such as northern Dauphin County. The "mobile" radios in vehicles work better, but the county's 1970−era system doesn't have enough channels to handle the emergency traffic, and different agencies often can't easily communicate with each other. Citing these and other problems, Dauphin County's commissioners are planning to spend as much as $35 million to replace the network. The commissioners expect to make a final decision next month, and at this point are leaning toward Motorola, which was recommended by a consultant and the county's emergency management personnel. Also being considered is M/A−Com Inc., which is doing the state's radio system as well as in Cumberland and Lebanon counties. Once the county approves a new system, it will be about three years until it is ready for use, officials said. Either option the county chooses will mean buying radios and pagers for police, fire and ambulance companies, which could cost $7 million to $11 million.
Source: http://www.pennlive.com/news/patriotnews/index.ssf?/base/news/1119518488194380.xml&coll=1

24. *June 23, Mississippi Press (MS)* — **Ham operators to show emergency skills.** When other means of communication are down in time of emergency, amateur radio operators provide a necessary service. Residents of Ocean Springs, MS, will have the opportunity at Field Day to meet and talk with local amateur radio operators, or "hams," to view their equipment, and to find out more about this radio service from noon Saturday, June 25, to noon Sunday, June 26, at Marshall Park in Ocean Springs. The Jackson County Amateur Radio Association will demonstrate emergency communications at the annual 24−hour event, which marks the end of Amateur Radio Week. The association's president, Don Wilson of WA5KNR, said he hopes the event creates awareness about amateur radio and its importance in everyday life, especially during hurricane season. With the slogan "Ham radio works when other systems don't," amateur radio operators use only generators, batteries or solar power, Wilson said. Hams construct emergency stations in parks, shopping malls and back yards to test their skills under all situations. They send messages in many forms without the use of phone systems, Internet, cell phones or other infrastructures that can be compromised in a crisis, he said.
Source: http://www.gulflive.com/news/mississippipress/index.ssf?/base/news/1119521766210970.xml

25. *June 22, Clay County Democrat (AR)* — **Arkansas first responders stage bioterrorism drill.** Members of the police and fire departments in Clay County, AR, along with public health professionals, Hazardous Materials teams, and an Air Evac Lifeteam, responded to a call for help at the Clay County Fairgrounds last Wednesday afternoon. Thankfully, it was just a drill. In the drill's scenario, children from the region are returning from an overnight school trip. While waiting for the children to board, the bus drivers are approached by several individuals with bags of helium balloons and cases of bottled drinks. The drivers are told a celebration surprise has been planned for the kids and are allowed to board the buses and release the balloons. The drinks are placed throughout the buses. The balloons contain VX and the drinks are also laced with this substance. During the ride home, the children start popping the balloons and those that are not popped begin deteriorating with an oily seepage onto the children. Some children begin coughing and develop various respiratory symptoms. The drill proceeds from this point. The county is required to hold one drill each year. This was classified as a bioterrorism drill due to the introduction of VX.
Source: http://www.claycountydemocrat.com/articles/2005/06/22/news/n ews4.txt

26. *June 22, Associated Press* — **Company urges replacement of police vests with Zylon.** Battered by lawsuits, the nation's top supplier of bullet−resistant police vests is urging its customers to replace vests containing the synthetic fiber Zylon, saying they may not be safe. Second Chance Body Armor Inc. said Wednesday, June 22, that tests suggested the vests "may fail to perform and result in serious injury or death." The company sent warnings to police agencies nationwide. The company previously recalled more than 130,000 vests made entirely with Zylon. The latest warning covers vests with filling blends containing any amount of the fiber, including about 58,000 Tri−Flex vests and an additional 40,000 Ultima and Ultimax vests with Performance Pacs. The vests are used by police officers and some government officials but not by the military. Toyobo Co., the Japanese manufacturer of Zylon, has acknowledged the fiber loses up to 20 percent of its durability within two years of manufacture. But the company said Zylon works well in body armor that is properly constructed, and is not to blame for any problems with Second Chance vests.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06 /22/AR2005062200769.html

[Return to top]

Information Technology and Telecommunications Sector

27. *June 23, Secunia* — **Cacti multiple unspecified vulnerabilities.** Some vulnerabilities have been reported in Cacti, which can be exploited by malicious people to conduct cross site scripting and SQL injection attacks or compromise a vulnerable system. Unspecified input is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Unspecified input is not properly sanitized before being used to include files. This can be exploited to include arbitrary files from external or local resources or execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 0.8.6e: http://www.cacti.net/download_cacti.php
Source: http://secunia.com/advisories/15490/

28.

June 22, SecurityFocus — **Ipswitch WhatsUp Professional LOGIN.ASP SQL injection vulnerability.** WhatsUp Professional is prone to an SQL injection vulnerability affecting its Web based front end. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. The vendor has released WhatsUp Professional 2005 SP1a to address this issue.
Source: http://www.securityfocus.com/bid/14039/discuss

29. *June 22, SecurityFocus* — **Veritas Backup Exec Admin Plus Pack Option remote heap overflow vulnerability.** Veritas Backup Exec is affected by a remote heap overflow vulnerability. A remote attacker can exploit this issue by crafting and sending malicious data to the service and executing arbitrary code. Successful exploitation may result in a super user compromise. Original advisory and updates: http://seer.support.veritas.com/docs/276607.htm
Source: http://www.securityfocus.com/bid/14023/solution

30. *June 22, SecurityFocus* — **Sun Java Web Start System property tags remote unauthorized access vulnerability.** A remote unauthorized access vulnerability affects Java Web Start. This issue is due to a failure of the application to properly validate user supplied input prior to considering it as trusted. An attacker may leverage this issue to gain unauthorized read and write access to affected computers. Other attacks may also be possible. It should be noted that unauthorized access granted in this way will be with the privileges of the unsuspecting user that visits a malicious Website. See Source link for solutions.
Source: http://www.securityfocus.com/bid/12847/solution

31. *June 22, CNET News* — **BlackBerry endures second outage in a week.** A number of BlackBerry handheld wireless devices experienced service problems on Wednesday, June 22, marking the second time in less than a week that the popular devices lost their data connections. A RIM representative said a hardware failure Wednesday triggered a backup system that operated at a lower capacity "than expected." Service has been restored, she said. BlackBerry customers, including a federal agency in Washington, DC, were told by RIM on Wednesday of an outage affecting accounts nationwide and across all carriers, according to an e−mail from RIM. Cell phone operator T−Mobile USA said an undisclosed number of its BlackBerry subscribers in Manhattan had only sporadic e−mail and other kinds of data service Wednesday. These problems were not related to what appears to be a nationwide Blackberry outage, according to a RIM representative.
Source: http://news.com.com/BlackBerry+endures+another+outage/2100−1039_3−5758043.html?tag=nefd.top

32. *June 22, Computerworld* — **Increased port 'sniffing' could herald attack, researcher warns.** An increase in "sniffing" activity on TCP Port 445 associated with a recently patched Microsoft vulnerability may be the signal of an impending attack attempting to exploit the flaw, according to an alert from analyst firm Gartner. The flaw in question is a remote code execution vulnerability associated with the Microsoft Windows Server Message Block (SMB) Protocol. Attackers who exploit this vulnerability could take complete control of affected systems. An increase in activity on TCP Port 445, which is associated with the SMB protocol, may be a signal that attackers are attempting to exploit the hole, Gartner analyst John Pescatore said in an alert posted Tuesday, June 21. Officials at Symantec also spotted increased activity on Port 445,

but they downplayed any immediate threat. Alfred Huger, senior director of engineering at Symantec, said his company noted a “significant spike” in activity last Friday, June 17. Since then, activity levels have gone back to normal. “Activity targeting Port 455 is very common. It’s almost like background noise,” Huger said. Companies that have installed Microsoft’s Windows XP SP2 should also be protected against the flaw because it closes off access to Port 445 by default, Huger said.
Source: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,102687,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US CERT reports a vulnerability in the Veritas NetBackup for NetWare Media Servers that could allow remote attackers to potentially crash the system. The vulnerability improperly handles request packets resulting in an unexpected error status value and can result in a crash of the program or a denial of service (DoS) condition. A hotfix has been developed for each of the affected versions. For more information on specific Veritas vulnerabilities please visit VERITAS Security Advisory VX05−008: Denial of Service (DoS) in VERITAS NetBackup for NetWare Media Servers at URL: * http://support.veritas.com/docs/277485

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 4004 (pxc−roid), 135 (epmap), 27015 (halflife), 1026 (−−−), 6881 (bittorrent), 53 (domain), 139 (netbios−ssn), 113 (auth), 4672 (eMule) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

33. *June 23, CBS News* — **Wildfires in western states.** Wildfires raced through a national forest in Arizona and a desert community in Southern California on Wednesday, June 22, burning

several homes and threatening hundreds more in an outbreak fueled by gusting winds and scorching temperatures. A grass fire in California raced through the Mojave Desert about 100 miles east of downtown Los Angeles in the Morongo Valley, an area that includes about 2,000 ranches and homes. Six homes and another building have been destroyed. The fire, aided by temperatures topping 100 degrees, created flames up to 30 feet high. About 300 firefighters were on the scene, supported by six airplanes and two helicopters. In Arizona, two lightning−caused brush fires forced the evacuation of at least 250 homes from a subdivision in the Tonto National Forest about 20 miles northeast of Phoenix. No injuries were reported, but television footage showed at least one structure on fire. The blazes grew to 12,500 acres during the afternoon and moved close to merging, although forest officials were unable to determine the exact acreage because of heavy smoke blanketing the sky. In Nevada, firefighters took advantage of calm winds to tame a fire that burned 750 acres near Carson City.
Source: http://www.cbsnews.com/stories/2005/06/23/national/main70362 3.shtml

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or

visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer